

## PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-269054

(43)Date of publication of application : 20.09.2002

(51)Int.Cl.

G06F 15/00  
H04L 9/32  
// G07B 15/00  
G07D 9/00

(21)Application number : 2001-071219

(71)Applicant : TIETECH CO LTD  
HASHIMOTO HIDENORI

(22)Date of filing : 13.03.2001

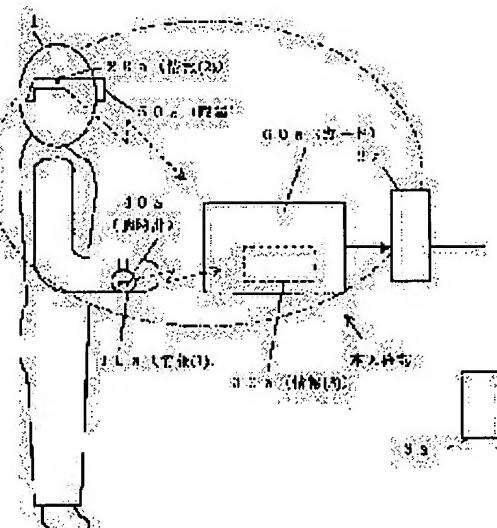
(72)Inventor : HASHIMOTO HIDENORI  
FUKATSU HIROICHI

## (54) IDENTIFYING DEVICE

## (57)Abstract:

PROBLEM TO BE SOLVED: To provide an identifying device which is low-cost and has high reliability.

SOLUTION: First and second user portable devices 10a and 20b provided to user portable equipments 40a and 50a that a user can carry and a user device 30a provided to a user device (card and portable telephone set) 60a that the user uses are used. One piece of information (original information) is divided on the whole to obtain 1st information (1), 2nd information (2), and 3rd information (3). The user portable device 10a holds the 1st information (1), the user portable device 20a holds the 2nd information (2), and the user device 30a holds the 3rd information (3). The user device 30a combines received information and the 3rd information (3) that the device itself has together by algorithm for processing. When the original information can be generated by combining the received information and the 3rd information (3) together, it is confirmed that the user is the original user of the user device 60a and the user is allowed to use the user device 60a.



(19) 日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2002-269054

(P2002-269054A)

(43) 公開日 平成14年9月20日 (2002.9.20)

(51) Int.Cl. <sup>7</sup>	識別記号	F I	テマコト <sup>*</sup> (参考)
G 06 F 15/00	3 3 0	C 06 F 15/00	3 3 0 C 3 E 0 4 0
H 04 L 9/32		C 07 B 15/00	5 1 0 5 B 0 8 5
// G 07 B 15/00	5 1 0	C 07 D 9/00	4 6 1 A 5 J 1 0 4
G 07 D 9/00	4 6 1	H 04 L 9/00	6 7 3 E

審査請求 未請求 請求項の数 6 OL (全 10 頁)

(21) 出願番号 特願2001-71219(P2001-71219)

(22) 出願日 平成13年3月13日(2001.3.13)

(71) 出願人 391006348

株式会社タイテック

愛知県名古屋市南区千種通2丁目13番地1

(71) 出願人 500200627

橋本 秀紀

東京都港区赤坂九丁目5番27号 ルピナス  
赤坂乃木坂302号

(72) 発明者 橋本 秀紀

東京都港区赤坂九丁目5番27号 ルピナス  
赤坂乃木坂302号

(74) 代理人 100064344

弁理士 岡田 英彦 (外3名)

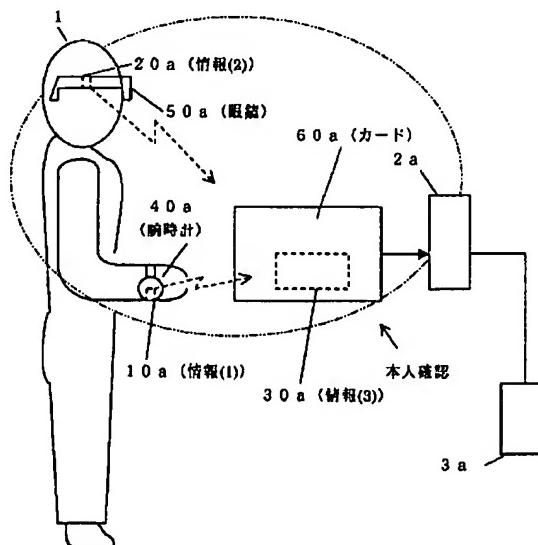
最終頁に続く

(54) 【発明の名称】 本人確認装置

(57) 【要約】

【課題】 低コストで、信頼性の高い本人確認装置を提供する。

【解決手段】 ユーザが携帯可能なユーザ携帯機器40a及び50aに設けられる第1及び第2のユーザ携帯装置10a及び20aと、ユーザが使用するユーザ機器(カードや携帯電話機)60aに設けられるユーザ装置30aを用いる。全体として一つの情報(原情報)を分割し、第1情報(1)、第2情報(2)、第3情報(3)を得る。ユーザ携帯装置10aに第1情報(1)を保有させ、ユーザ携帯装置20aに第2情報(2)を保有させ、ユーザ装置30aに第3情報(3)を保有させる。ユーザ装置30aは、受信した情報と自身が保有する第3情報(3)を処置のアルゴリズムで結合する。そして、受信した情報と第3情報(3)を結合して原情報を成すことができた場合には、ユーザ1がユーザ機器60aの本来のユーザであることを確認し、ユーザ機器60aの使用を可能とする。



【特許請求の範囲】

【請求項1】 ユーザ機器を使用する人がそのユーザ機器の本来のユーザであることを確認する本人確認装置であって、  
ユーザが携帯する少なくとも第1及び第2のユーザ携帯装置と、  
ユーザが使用するユーザ機器に設けられるユーザ装置とを備え、  
第1のユーザ携帯装置は、原情報を分割して得た少なくとも第1～第3情報のうちの第1情報を記憶する第1記憶手段と、第1記憶手段に記憶されている第1情報を送信する第1通信手段とを有し、  
第2のユーザ携帯装置は、原情報を分割して得た少なくとも第1～第3情報のうちの第2情報を記憶する第2記憶手段と、第2記憶手段に記憶されている第2情報を送信する第2通信手段とを有し、  
ユーザ装置は、原情報を分割して得た少なくとも第1～第3情報のうちの第3情報を記憶する第3記憶手段と、第3通信手段と、第3通信手段で受信した情報と第3記憶手段に記憶している第3情報を結合し、原情報を形成することができた場合に本人であることを確認する本人確認手段とを有する、本人確認装置。  
【請求項2】 請求項1に記載の本人確認装置であって、第1及び第2のユーザ携帯装置は、所定時間毎に第1情報を送信する、本人確認装置。  
【請求項3】 請求項1に記載の本人確認装置であって、  
ユーザ装置は、情報送信要求信号を送信し、  
第1及び第2のユーザ携帯装置は、情報送信要求信号を受信した時に第1情報を第2情報を送信する、本人確認装置。  
【請求項4】 請求項1～3のいずれかに記載の本人確認装置であって、ユーザ機器には、第3情報の不正な読み出しを検出した時に、第3情報の読み出しを禁止する読み出禁止手段が設けられている、本人確認装置。  
【請求項5】 請求項4に記載の本人確認装置であって、読み出禁止手段は、第3記憶手段を破壊する、本人確認装置。  
【請求項6】 請求項1～5のいずれかに記載の本人確認装置であって、本人確認手段は、本人であることを確認した場合にユーザ機器の使用を許可する、本人確認装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、ユーザ機器を使用するユーザがそのユーザ機器の本来のユーザであることを（本人であること）を確認する本人確認装置に関する。特に、認証が必要であるシステムに好適に用いることができる本人確認装置に関する。

【0002】

【従来の技術】ユーザがサービス会社のサービスを利用する場合、サービス会社は、サービスを利用しようとするユーザが本人であることを確認するために、認証を行っている。認証方法としては、例えば、暗証番号を用いる方法、サイン用いる方法、印章を用いる方法、IDコード（非接触でユーザ機器へIDコードを送信または送受信する小型通信機）を用いる方法等が使用されている。暗証番号を用いる方法は、例えば、キャッシュカードを用いて銀行の口座から現金を引き出す場合に用いられる。ユーザは、現金を引き出す場合、銀行のATM（現金自動支払機）のカード挿入口にキャッシングカードを挿入し、暗証番号を入力する。ATMは、キャッシングカードから読み取ったカード情報（例えば、ID）とユーザが入力した暗証番号を認証センタに送信する。認証センタは、ATMに入力された暗証番号及び読み取ったカード情報と、記憶手段に記憶されているカード情報と暗証番号との対応関係を含むデータベースに基づいて、認証を行う。サインを用いる方法は、例えば、クレジットカードを用いて商品の代金を支払う場合に用いられる。ユーザは、クレジットカードで代金を支払う場合、商品購入票にサインをする。商品販売者は、商品購入票のサインとクレジットカードに記入されているサインを比較することによって認証を行う。印章を用いる方法は、例えば、預金通帳を用いて銀行の口座から現金を引き出す場合に用いられる。ユーザは、預金通帳を用いて銀行の口座から現金を引き出す場合、現金引出用紙に印鑑を用いて押印する。銀行は、現金引出用紙に押印された印章と予め登録されている印章とを比較することによって認証を行う。IDコードを用いる方法は、例えば、ユーザが使用するユーザ機器の不正使用を防止する場合等に用いられる。この方法では、ユーザが携帯するタグ（送受信機能付きのカード部材等）及びユーザが使用するユーザ機器（例えば、携帯電話）に同じIDコードを記憶させる。タグは、ユーザ機器に接続して使用することもできるが、無線タグとして使用する場合が多い。ユーザ機器は、タグから送信されたIDコードと自己が記憶しているIDコードとを照合し、一致している場合にはユーザ機器の使用制限を解除（使用許可信号を出力）する。また、ユーザ本人であることを確認する他の認証方法として、各人に固有の生体情報（声紋、指紋、掌紋、網膜パターン、顔を撮像した画像等）を用いる方法が知られている。この認証方法では、生体情報読取装置によってユーザの生体情報を読み取り、読み取った生体情報と予め登録されている生体情報とを照合することによって認証を行うものである。この認証方法は、各人に固有の生体情報を用いるため、認証精度が高い。

【0003】

【発明が解決しようとする課題】暗証番号、サイン、印章やIDコードによって本人確認を行う従来の本人確認方法は、キャッシングカードを使用した人、クレジットカ

ードを使用した人、預金通帳を使用した人、IDコードを記憶させたタグを携帯する人が本来のユーザでない場合でも、正しいユーザであると認証してしまうことがある。例えば、ユーザ機器（例えば、キャッシュカード）や印鑑等の盗難、暗証番号、サインやIDコード等の情報盗難や情報漏洩が発生すると、ユーザ機器が不正使用されてしまう。また、生体情報によって本人確認を行う従来の本人確認方法は、生体情報読取装置（例えば、撮像手段）や生体情報処理装置（例えば、画像処理装置、大容量の記憶装置）等が必要であるため、システム全体のコストが高くなる。また、指に傷がついた場合や眼病になった場合には、指紋や網膜パターンが変化し、認証精度が低下する可能性がある。また、網膜パターンを用いる場合には、目を測定位置に持って行く必要があるため、煩わしさがある。また、指紋を用いる場合には、指を指紋読取装置に接触させる必要があるため、きれい好きの人にとっては心理的不快感がある。そこで、本発明は、低コストで信頼性の高い本人確認装置を提供することを目的とする。

#### 【0004】

【課題を解決するための手段】前記課題を解決するための本発明の第1発明は、請求項1に記載されたとおりの本人確認装置である。請求項1に記載の本人確認装置では、原情報を少なくとも第1～第3情報を分割し、第1情報をユーザが携帯する第1のユーザ携帯装置に記憶させ、第2情報をユーザが携帯する第2のユーザ携帯装置に記憶させ、第3情報をユーザが使用するユーザ機器に設けられるユーザ装置に記憶させ、ユーザ装置は、受信した情報と自分が保有している情報を結合して原情報を形成することができた場合に、本人であることを確認する。請求項1に記載の本人確認装置を用いれば、生体情報を用いる場合に比べて安価に構成することができ、暗証番号やカードを盗まれても不正使用の心配がない。また、第1及び第2のユーザ携帯装置とユーザ装置には原情報を分割した第1～第3情報を記憶させている（同じ情報でない）ため、ユーザ使用機器が盗まれても不正使用の心配がない。これにより、暗証番号、サイン、印鑑、IDコード等を用いる場合に比べて信頼性が高い。また、本発明の第2発明は、請求項2に記載されたとおりの本人確認装置である。請求項2に記載の本人確認装置を用いれば、第1及び第2のユーザ携帯装置は、所定時間毎に第1情報を及び第2情報を送信するため、ユーザ装置は、本人であるか否かを常時確認することができる。また、本発明の第3発明は、請求項3に記載されたとおりの本人確認装置である。請求項3に記載の本人確認装置では、ユーザ装置は、例えば、本人確認を行う必要がある時に、第1及び第2のユーザ携帯装置に情報送信要求信号を送信し、第1及び第2のユーザ携帯装置から第1情報を及び第2情報を受信する。これにより、第1及び第2のユーザ携帯装置の消費電力を低減するこ

ができる。また、本発明の第4発明は、請求項4に記載されたとおりの本人確認装置である。請求項4に記載の本人確認装置では、ユーザ機器には、ユーザ装置に記憶されている第3情報の不正な読み出しを検出した時に第3情報の読み出しを禁止する読み出禁止手段が設けられている。これにより、第3情報が不正に読み出されるのを防止することができ、信頼性が一層向上する。また、本発明の第5発明は、請求項5に記載されたとおりの本人確認装置である。請求項5に記載の本人確認装置では、読み出禁止手段は、第3記憶手段を破壊する。このため、簡単な構成で、ユーザ装置に記憶されている第3情報が不正に読み取られるのを防止することができる。また、本発明の第6発明は、請求項6に記載されたとおりの本人確認装置である。請求項6に記載の本人確認装置を用いれば、本人確認手段が本人であることを確認した場合のみ、ユーザ機器の使用が可能となるため、信頼性が向上する。

#### 【0005】

【発明の実施の形態】以下に、本発明の実施の形態を図面を参照して説明する。本発明に対応する本人確認方法の第1の実施の形態の概略図を図1に示す。なお、図1は、本発明の本人確認方法を用いて認証システムを構成した図を示している。例えば、ユーザ1が、ユーザ機器の一種であるデビットカード60aを用いて決済を行う場合（購入品の代金の支払い）、従来の認証方法では、以下のようにしてユーザ認証が行われる。まず、ユーザ1は、デビットカード60aを認証端末装置2aのカード挿入口に挿入するとともに、暗証番号を入力手段等を用いて入力する。認証端末装置2aは、デビットカード60aに記憶されているカード情報（ID等）を読み取り、読み取ったカード情報と、ユーザ1が入力した暗証番号を含むユーザ情報を認証センタ3aに送信する。認証センタ3aは、認証端末装置2aから送信されたカード情報及び暗証番号と、暗証番号をカード情報に対応させて記憶しているデータベースとを照合することによって認証を行う。そして、認証センタ3aは、認証がOKであれば、認証OK信号を認証端末装置2aに送信し、認証がNGであれば、認証NG信号を認証端末装置2aに送信する。

【0006】この認証処理では、前述したように、ユーザ1がデビットカード60aの本来のユーザであることの確認（本人確認）は行われていない。そこで、本実施の形態では、認証センタ3aでユーザ認証処理が行われる前に、本人確認処理（図1の二点鎖線で囲んだ部分）が以下のように行われる。本実施の形態では、本人確認装置は、少なくとも、ユーザ1が携帯する第1ユーザ携帯機器40aに設けられたユーザ携帯装置10aと、第2ユーザ携帯機器50aに設けられたユーザ携帯装置20aと、ユーザが使用するユーザ機器60aに設けられたユーザ装置30aにより構成される。第1及び第2の

ユーザ携帯装置10aとユーザ装置30aは、例えば、ユーザ認証を行うサービス会社が用意する。ユーザ携帯装置10a、20a、ユーザ装置30aを、ユーザ携帯機器40a、50a、ユーザ機器60aに取り付ける方法は種々の方法が可能である。例えば、接着剤や接着テープ等の取付手段を用いる方法、第1及び第2のユーザ携帯機器40a及び50aやユーザ機器60aに内蔵する方法等を用いることができる。また、本実施の形態では、ユーザ装置30aは、例えば、本人であることを確認できるまでは、使用禁止信号を出力してユーザ機器であるデビットカード60aを使用不能状態とする。すなわち、認証端末装置2aがデビットカード60aのカード情報を読み出すことができないようにする。

【0007】第1及び第2のユーザ携帯装置10a及び20aとユーザ装置30aには、本人確認に必要な情報が記憶されている。例えば、元々一つの情報として認識される情報（原情報）を少なくとも3つの情報に分割し、第1の分割情報（第1情報(1)）を第1のユーザ携帯機器40a（例えば、腕時計）に設けられるユーザ携帯装置（10a）に保有（記憶）させ、第2の分割情報（第2情報(2)）を第2のユーザ携帯機器50a（例えば、眼鏡）に設けられる第2のユーザ携帯装置（10a）に保有（記憶）させ、第3の分割情報（第3情報(3)）をユーザ機器60a（例えば、デビットカード）に設けられるユーザ装置30aに保有（記憶）させる。原情報を分割する方法としては、種々の方法を用いることができる。

【0008】なお、第1及び第2ユーザ携帯機器40a及び50aは、腕時計や眼鏡に限定されず、ユーザ1が携帯可能あるいは携行可能であればよい。例えば、指輪、眼鏡、ベルトのバックル、ブレスレッド、ペンダント、イアリング、財布、定期券、免許証等を用いることができる。また、第1及び第2ユーザ携帯機器40a及び50aは同じユーザ携帯機器を用いてもよい。また、第1及び第2のユーザ端末装置10a及び20aは、ユーザ携帯機器40a及び50aと共に携帯する必要はなく、例えば、財布、カバンやポケットに入れて携帯してもよい。また、ユーザ機器60aは、カードに限定されず、本人確認が必要な機器であればよい。例えば、携帯電話やパソコン等でもよい。ユーザ機器60aは、複数のユーザが共用するものであってもよい。また、携帯電話機以外の、通信機能を備える、PHS（Personal Handphone System）電話機、PDA（Personal Data Assistance、個人用携帯情報端末）無線機、ETC（Electronic Toll Collection System、ノンストップ自動料金支払システム）用通信機、ITS（Intelligent Transport Systems、高度道路交通システム）用の車両通信機、電話通信端末（例、公衆電話機、FAX端末）、データ通信端末（例、パソコン）等を用いることができる。何をユーザ機器として用いるかは、営業上または設

計上の選択事項である。第1及び第2ユーザ携帯装置10a及び20aは、第1情報(1)及び第2情報(2)をユーザ装置30aに送信する送信手段を備えている。第1情報(1)及び第2情報(2)を送信する方法としては、無線電波を用いてもよいし、超音波や光（赤外線）を用いてもよい。

【0009】ユーザ装置30aは、第1情報(1)及び第2情報(2)を受信すると、受信した第1情報(1)及び第2情報(2)と自身が記憶している第3情報(3)を所定のアルゴリズムで結合して情報(4)を作成（形成）する。そして、情報(4)と原情報を照合することによって本人確認を行う。すなわち、受信した第1情報(1)と第2情報(2)と自身が記憶している情報(3)を用いて原情報を再生あるいは復元することができた場合に、本人であることを確認する。前記したように、対応する第1及び第2のユーザ携帯装置10a及び20aとユーザ装置30aには、同一の原情報から生成された分割情報（第1情報(1)、第2情報(2)、第3情報(3)）を記憶させている。このため、ユーザ装置30aは、正しい第1情報(1)及び第2情報(2)を受信した場合にだけ、原情報を再生あるいは復元することができる。図1に示す認証システムでは、ユーザ機器であるデビットカード60aは、ユーザ1が本人であることを確認した場合にのみ、自身が記憶しているカード情報を認証端末装置2aで読み取り可能とする。以上のように、デビットカード60aは、本人確認処理を行った後に、自身が記憶しているカード情報を認証端末装置2aに出力するように構成されている。ここで、デビットカード60aを紛失し、盗まれ、あるいは、暗証番号を他人に知られた場合には、デビットカード60aは、そのデビットカード60aの本来のユーザが携帯している第1及び第2のユーザ携帯装置10a及び20aから送信される第1情報(1)及び第2情報(2)を受信することができない。このため、認証センタ3aでユーザ認証が行われる前に、ユーザ装置30aの本人確認処理によって不正使用を確実に阻止することができる。

【0010】本実施の形態では、割り符のように、一つの原情報を少なくとも第1情報(1)と第2情報(2)と第3情報(3)に分割し、第1情報(1)を第1のユーザ携帯装置10aに記憶させ、第2情報(2)を第2のユーザ携帯装置20aに記憶させ、第3情報(3)をユーザ装置30aに記憶させている。そして、ユーザ装置30aは、正しい第1情報(1)及び第2情報(2)を受信した時に本人であることを確認する。したがって、生体情報を用いる場合に比して、安価に構成することができる。また、暗証番号やカードを盗まれたり、紛失したりしても、ユーザ携帯機器（ユーザ携帯装置）を盗まれたり、紛失したりしない限り、不正使用の心配がない。また、第1及び第2のユーザ携帯装置10a及び20aとユーザ装置30aには異なる情報を記憶させているので、いずれかが盗ま

れたり、紛失しても不正使用の心配がない。したがって、暗証番号、サイン、IDデータ等を用いる場合に比べて、確実に本人確認を行うことができる。なお、本発明は、ユーザがユーザ機器を使用する際に、ユーザがそのユーザ機器の本当のユーザであるか否かを確認（本人確認）するための方法に関するものである。したがって、ユーザ機器（ユーザ装置）で本人確認処理を行った結果をどのように利用するかは、ユーザ機器の種類やユーザ機器を利用する形態に応じて適宜選択される事項である。例えば、図1では、ユーザ装置30aは、本人であることを確認すると、デビットカード（ユーザ機器）60aのカード情報の認証端末装置2aへの出力を許可する。これにより、デビットカード60aのカード情報が認証端末装置2aで読み取られる。また、ユーザ1は、認証端末装置2aの入力手段等を用いて暗証番号を入力する。以後は、従来例と同様の手順で、認証センタ3aでユーザ認証処理（デビットカードの正当性を認証する処理）を行う。

【0011】次に、本実施の形態の本人確認装置を用いて本人確認処理を行う場合の手順を説明する。図2は、本人確認方法の処理手順の1例を説明する図である。本実施例では、ユーザ装置30は、常時本人確認処理を行う。本実施例では、①～⑩の手順で本人確認処理が行われる。

①ユーザ携帯装置10は、適宜の時期に（例えば、所定の時間間隔で）、自身が保有（記憶）している第1情報(1)を送信する。

②ユーザ携帯装置20は、適宜の時期に（例えば、所定時間間隔で）自身が保有（記憶）している第2情報(2)を送信する。ここで、情報の送信方法によっては、ユーザ携帯装置10及び20が同時に情報を送信すると、双方の情報が干渉してユーザ装置30で情報を正確に受信できなくなる可能性がある。そこで、ユーザ携帯装置10の送信時期とユーザ携帯装置20の送信時期が重ならないように設定するのが好ましい。例えば、ユーザ携帯装置10とユーザ携帯装置20が送信する時期を予め設定しておく。

③受信待機状態にあるユーザ装置30は、第1情報(1)及び第2情報(2)を受信する。

④ユーザ装置30は、第1情報(1)及び第2情報(2)を受信すると、受信した第1情報(1)及び第2情報(2)と自身が保有（記憶）している第3情報(3)を所定のアルゴリズムで結合して第4情報(4)を形成する。

⑤ユーザ装置30は、情報(4)と原情報を照合して、情報(4)と原情報が一致した場合（第1情報(1)と第2情報(2)と第3情報(3)を結合して原情報を形成することができた場合）には、ユーザが本人であることを確認する。

【0012】図3は、本発明の本人確認方法の処理手順の他の例を説明する図である。本実施例では、ユーザ装置30は、本人確認が必要な場合に本人確認処理を行

う。本実施例では、①～⑩の手順で本人確認処理が行われる。

①ユーザ装置30は、本人確認処理を行う必要がある場合（例えば、デビットカードが認証端末装置のカード挿入口に挿入された場合等）に、情報の送信要求信号を送信する。

②受信待機状態にあるユーザ携帯装置10は、送信要求信号を受信する。

③ユーザ携帯装置10は、送信要求信号を受信すると、自身が記憶している第1情報(1)を送信する。

④受信待機状態にあるユーザ携帯装置20は、送信要求信号を受信する。

⑤ユーザ携帯装置20は、送信要求信号を受信すると、自身が記憶している第2情報(2)を送信する。ここで、情報の送信方法によっては、ユーザ携帯装置10及び20が同時に情報を送信すると、双方の情報が干渉してユーザ装置30で情報を正確に受信できなくなる可能性がある。そこで、ユーザ携帯装置10の送信時期とユーザ携帯装置20の送信時期が重ならないように設定するのが好ましい。例えば、送信要求信号を受信してからそれぞれ異なる待機時間が経過した後に情報を送信するように設定する。あるいは、ユーザ装置30からユーザ携帯装置10あるいはユーザ携帯装置に異なる時間に送信要求信号を送信する。

⑥受信待機状態にあるユーザ装置30は、第1情報(1)と第2情報(2)を受信する。

⑦ユーザ装置30は、受信した第1情報(1)及び第2情報(2)と自身が保有（記憶）している第3情報(3)を所定のアルゴリズムで結合して情報(4)を形成する。

⑧ユーザ装置30は、情報(4)と原情報を照合し、情報(4)が原情報と一致する場合に、本人であることを確認する。

なお、ユーザ装置30は、第1情報(1)及び第2情報(2)を受信できない場合、または、受信した情報が第1情報(1)あるいは第2情報(2)でない場合には、所定の処理を実行する。例えば、送信要求信号を送信した後、所定時間内に情報を受信できない場合には、再度送信要求信号を送信する。そして、所定回数送信要求信号を送信しても情報を受信できない場合には、本人を確認できないと判断し、所定の終了処理を実行する。例えば、エラーメッセージを認証端末装置に表示させる。

【0013】次に、原情報を分割、結合する方法を図4により具体的に説明する。本実施例では、原情報「数字7の図形のビット行列」を、左右に引いた2つの分割線(1)及び分割線(2)を境に、上部の第1情報(1)と中央の第2情報(2)と下部の第3情報(3)に分割する。そして、第1情報(1)をユーザ携帯装置10に記憶させ、第2情報(2)をユーザ携帯装置20に記憶させ、第3情報(3)及び原情報をユーザ装置30に記憶させる。ユーザ装置30は、情報を受信すると、受信した情報と自身が記憶し

ている第3情報(3)を所定のアルゴリズムで結合して情報(4)を形成する。本実施例では、受信した情報のビット行列と第3情報(3)のビット行列を結合する。受信した情報が第1情報(1)及び第2情報(2)の場合には、受信した情報のビット行列と第3情報(3)のビット行列を結合すると、原情報【数字7の図形のビット行列】が形成される。さらに、情報(4)と原情報を照合して本人確認を行う。本実施例では、情報(4)のビット行列で表される図形が、原情報のビット行列で表される図形と同じであるか否かを判断する。分割線を引く場所、引き方、分割線の本数等は、適宜選択可能である。受信した情報と自分が記憶している情報を結合するアルゴリズムは、原情報を分割する分割方法によって決定される。

【0014】次に、本発明の本人確認装置の第1の実施の形態のプロック図を図5に示す。本実施の形態の本人確認装置は、第1のユーザ携帯装置10bと第2のユーザ携帯装置20bとユーザ装置30bにより構成されている。第1のユーザ携帯装置10bは、信号出力手段11b、変調／復調手段12b、通信手段(第1の通信手段)13bにより構成されている。信号出力手段11bは、例えば、第1情報(1)を記憶する記憶手段(第1記憶手段)を有し、第1情報(1)を出力する。記憶手段に記憶する第1情報(1)の形式としては、種々の形式を用いることができる。変調／復調手段12bは、信号出力手段11bから出力された第1情報(1)を変調し、通信手段13bを介して送信する。あるいは、変調／復調手段12bは、通信手段13bを介して受信した信号を復調する。そして、復調した信号に送信要求信号が含まれている場合には、第1情報(1)を変調し、通信手段13bを介して送信する。ユーザ携帯装置10bには、各手段に電力を供給する電池が設けられている。第2のユーザ携帯装置20bは、第1のユーザ形態装置10bと同じ構成であり、信号出力手段21b、変調／復調手段22b、通信手段(第2の通信手段)23bにより構成されている。信号出力手段21bは、第2情報(2)を記憶する記憶手段(第2記憶手段)を有し、第2情報(2)を出力する。変調／復調手段22bは、信号出力手段21bから出力された第2情報(2)を変調し、通信手段23bを介して送信する。あるいは、変調／復調手段22bは、通信手段23bを介して受信した信号を復調する。そして、復調した信号に送信要求信号が含まれている場合には、第2情報(2)を変調し、通信手段23bを介して送信する。ユーザ携帯装置20bには、各手段に電力を供給する電池が設けられている。

【0015】ユーザ装置30bは、通信手段(第3の通信手段)31b、変調／復調手段32b、結合手段33b、信号出力手段34bを有している。変調／復調手段32bは、通信手段31bを介して受信した信号を復調し、結合手段33bに出力する。あるいは、変調／復調手段32bは、送信要求信号を変調し、通信手段31b

を介して送信する。そして、その後に通信手段31bを介して受信した信号を復調し、結合手段33bに出力する。信号出力手段34bは、第3情報(3)を記憶する記憶手段(第3記憶手段)を有し、第3情報(3)を出力する。結合手段33b(本人確認手段)は、復調／変調手段32bから入力された信号(第1情報(1)と第2情報(2))と第3情報(3)を所定のアルゴリズムで結合して情報(4)を形成する。例えば、割り符を合わせる方法を用いて第1情報(1)と第2情報(2)と第3情報(3)を結合する。さらに、結合手段33bは、情報(4)と原情報の照合結果に基づいて本人か否かを確認する。結合手段33bは、信号出力手段34bあるいは変調／復調手段32bと一緒に設けてもよい。ユーザ装置30bには、各手段に電力を供給する電池が設けられている。結合手段33bは、例えば、本人が確認されない時には出力禁止信号を出力する。結合手段33bから出力禁止信号が出力されていると、ユーザ機器は使用不能となる。例えば、デビットカードに記憶されているカード情報を認証端末装置で読み取ることができない、あるいは携帯電話機を使用することができない。なお、原情報は、ユーザ装置30bの出力手段34bに記憶させてもよい。

【0016】ユーザ装置とユーザ機器が別体の場合には、ユーザ装置(結合手段)とユーザ機器との間の信号の伝送は、無線あるいはケーブルを介して行われる。なお、ユーザ装置及びユーザ機器に互いに接続可能な接続端子を設けておけば、接続端子同士を接続するだけでユーザ装置とユーザ機器を接続することができるため、接続作業が容易となる。なお、ユーザ携帯装置10b、20bの信号出力手段11b、21b、変調／復調手段12b、22b、ユーザ装置30bの信号出力手段34b、変調／復調手段32b、結合手段33b、信号出力手段34bは、ハードウェアで実現してもよいし、ソフトウェアで実現してもよい。本実施の形態の結合手段33bが、本発明の本人確認手段に対応する。

【0017】図6は、ユーザ機器60bの1実施例の斜視図である。図6に示すユーザ機器60bは、カード状に形成されている。そして、カードの内部に、図5に示した各手段31b～34bが設けられている。ユーザ機器60bは、ユーザ携帯装置10b及び20bと通信を行う通信機能を備えた通信機器である。ユーザ機器60bとしては、磁気カード、ICカード、デビットカード、クレディットカード、キャッシュカード等を用いることもできる。例えば、デビットカード、クレディットカードまたはキャッシュカード等の決済用カードに通信手段を設けることによって、決済用カードに本人確認機能を持たせることができる。なお、カードは、決済用カードや金融用カードに限定されるものではなく、無線機等の通信機器をカード状に形成したものでもよいことは、勿論である。

【0018】図7は、本発明の本人確認装置の第2の実

施の形態のブロック図である。本実施の形態では、ユーザ装置30c（例えば、信号出力手段34c）に、破壊手段36cを設けている。破壊手段36cは、所定の情報（例えば、信号出力手段34cに記憶されている第3情報(3)）の不正な読み出しを検出した場合に、信号出力手段34cから所定の情報が外部に出力されるのを阻止する。不正な読み出しの検出は、例えば、通信手段31cで受信した信号に、正規の読み出し信号以外の読み出し信号が含まれていることにより検出する。信号出力手段34cからの信号出力を阻止する方法としては、例えば、信号出力手段34cに過電流を流し、信号出力手段34cを破壊する方法を用いることができる。あるいは、揮発性の記憶手段に情報等を記憶させている場合には、記憶手段への電源供給を遮断し、記憶手段に記憶されている情報等を消去する方法を用いてもよい。なお、破壊手段36cは、ユーザ装置30cが分解されることを検出した場合に、信号出力手段34cあるいはユーザ装置30cを破壊するものでもよい。本実施の形態の破壊手段36cが、本発明の読み出禁止手段に対応する。

## 【0019】

【発明の効果】本発明は、以下に記載する効果を有する。本発明は、生体情報、暗証番号、サイン（署名）、印章あるいはIDコード等を用いるのではなく、割り符のような、元々は一つの情報または信号を分割した情報を用いている。そして、各分割情報を、ユーザが携帯するユーザ携帯装置とユーザが使用するユーザ機器に設けられるユーザ装置にそれぞれ保持させ、ユーザ携帯装置とユーザ装置が保持している情報を結合（割り合せ）を行って本人確認を行っている。このような情報は、生体情報のように変動することがない。また、通信手段や各情報の結合手段等は、ICチップ等によって簡単に、安価に構成することができる。したがって、精度が高く、かつ低成本で本人確認を行うことができる。また、本発明では、ユーザ携帯装置が保有している情報とユーザ機器で保有している情報が結合されて元の情報（原情報）が復元されない限り、本人確認が行われない。このため、暗証番号やカードやIDタグ等を盗まれても不正使用の心配がない。つまり、ユーザ装置及びユーザ携帯装置を落としたり、盗まれたりしない限り、不正使用の恐れはない。ユーザ携帯装置をICチップで構成すれば、ユーザが携帯可能な多くの部材（例えば、指輪やメガネ）に取り付けることができる。この場合、ユーザ携帯機器を、ユーザが自分で決めた部材に取り付けることができるので、ユーザ携帯機器が盗まれる恐れもほとんどない。本発明では、2台以上のユーザ携帯装置に分割情報を記憶させているため、不正使用の恐れは一層少ない。万一、情報が漏れている恐れがある場合には、ユーザ携帯機器及びユーザ機器の所定のICチップを新たなチップに交換すればよい。以上のように、本発明を用いることにより、不特定多数のユーザに対して、

簡単、低成本、高信頼性、高セキュリティで本人確認処理を行うことができる。

【0020】本発明は、前記した実施例の構成に限定されることなく、本発明の要旨を変更しない範囲で種々の変更、追加、削除が可能である。例えば、ユーザ装置とユーザ機器との組付け形態、ユーザ携帯装置とユーザ携帯機器との組付け形態は、一体構成あるいは別体構成等種々変更可能である。例えば、ユーザ携帯装置をICチップで形成するとともに、ICチップをユーザ携帯機器（腕時計、眼鏡等）に接着剤や接着テープ等によって貼り付けることもできる。また、ユーザ装置とユーザ機器を一体に構成することもできる。また、ユーザ装置を構成する手段をユーザ機器を構成する手段と兼用してもよい。なお、ユーザ携帯装置がユーザ携帯機器に一体化的に設けられている場合、ユーザ装置がユーザ機器に一体化的に設けられている場合には、ユーザ携帯装置及びユーザ装置は、それぞれユーザ携帯機器及びユーザ機器ということもできる。また、ユーザ携帯装置とユーザ装置との間の情報の送受信を非接触で行ったが、接触させた状態で情報の送受信をおこなうこともできる。また、2台のユーザ携帯装置と1台のユーザ装置により本人確認装置を構成したが、ユーザ携帯装置の数は3以上でもよい。この場合には、本発明は、例えば、「原情報を分割してN個（Nは3以上の整数）の分割情報を形成し、第1分割情報～第(N-1)分割情報をそれぞれ第1ユーザ携帯装置～第(N-1)ユーザ携帯装置に記憶させるとともに、第N分割情報をユーザ装置に記憶させ、ユーザ装置（本人確認手段）は、受信した情報を所定のアルゴリズムで結合して原情報を形成することができた場合にユーザがそのユーザ機器の本来のユーザであることを確認する本人つかい忍装置。」として構成することができる。また、ユーザ携帯装置とユーザ装置との間で情報を伝送する際に情報が漏洩するのを防止する方法を用いることもできる。例えば、送信側に、情報を暗号化する暗号化手段を設け、受信側に、暗号化された情報を解読する暗号解読手段を設ける。あるいは、送信側に、情報にランダムノイズ(RN)を挿入するRN挿入手段を設け、受信側に、RNが挿入された情報からRNを除去するRN除去手段を設ける。また、本発明は本人確認方法として構成することもできる。

【0021】以上説明したように、請求項1～6に記載の本人確認装置を用いれば、安価に、高い信頼性で本人を確認することができる。

## 【図面の簡単な説明】

【図1】本発明の本人確認方法の一実施の形態の概略図である。

【図2】本発明の本人確認方法の処理手順の1例を説明する図である。

【図3】本発明の本人確認方法の処理手順の他の例を説明する図である。

【図4】原情報を分割する1例を説明する図である。  
【図5】本発明の本人確認装置の第1の実施の形態のブロック図である。

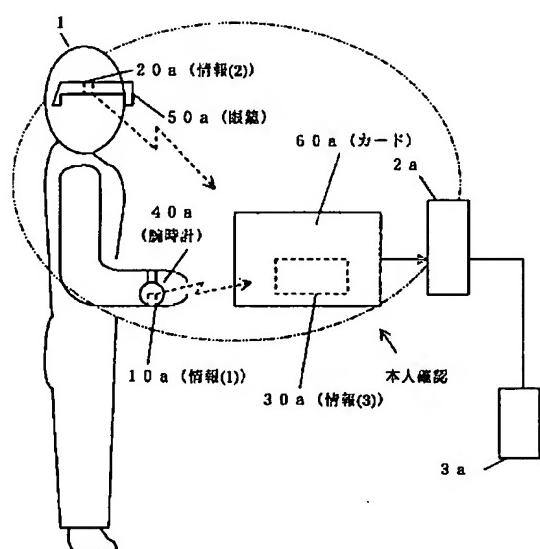
【図6】ユーザ機器の1実施例を示す図である。  
【図7】本発明の本人確認装置の第2の実施の形態のブロック図である。

【符号の説明】

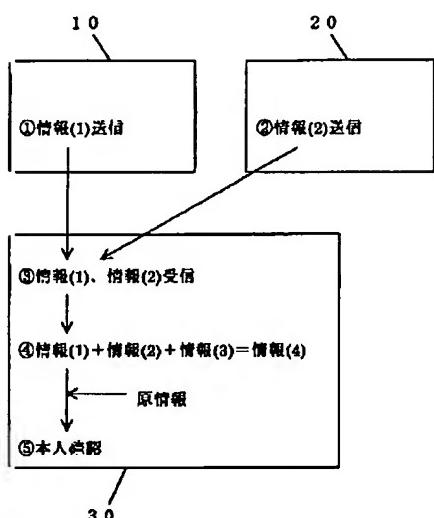
- 1 ユーザ
- 2 a 認証端末装置
- 3 a 認証センタ
- 10、10 a～10 c、20、20 a～20 c ユーザ携帯装置

- 11 b、11 c、21 b、21 c 信号出力手段
- 12 b、12 c、22 b、22 c 変調／復調手段
- 13 b、13 c、23 b、23 c 通信手段
- 30、30 a～30 c、ユーザ装置
- 31 b、31 c 通信手段
- 32 b、32 c 変調／復調手段
- 33 b、33 c 結合手段（本人確認手段）
- 34 b、34 c 信号出力手段
- 36 c 破壊手段（読み出禁止手段）
- 40 a、50 a ユーザ携帯機器
- 60 a、60 b ユーザ機器

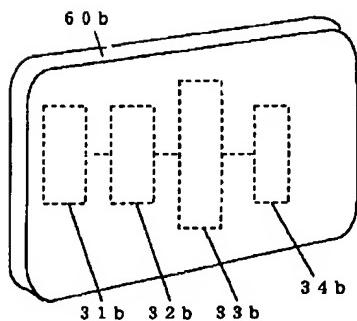
【図1】



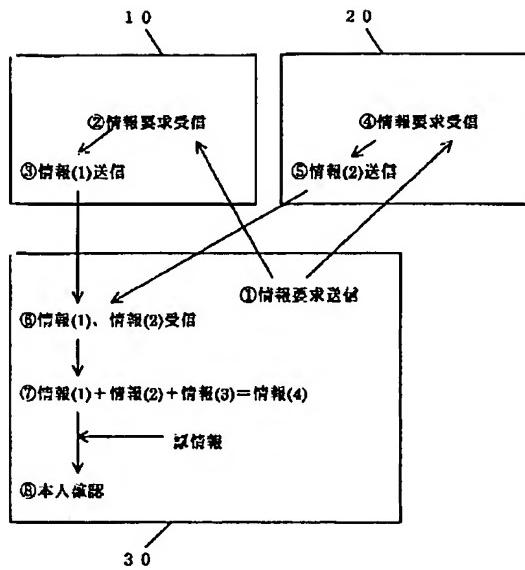
【図2】



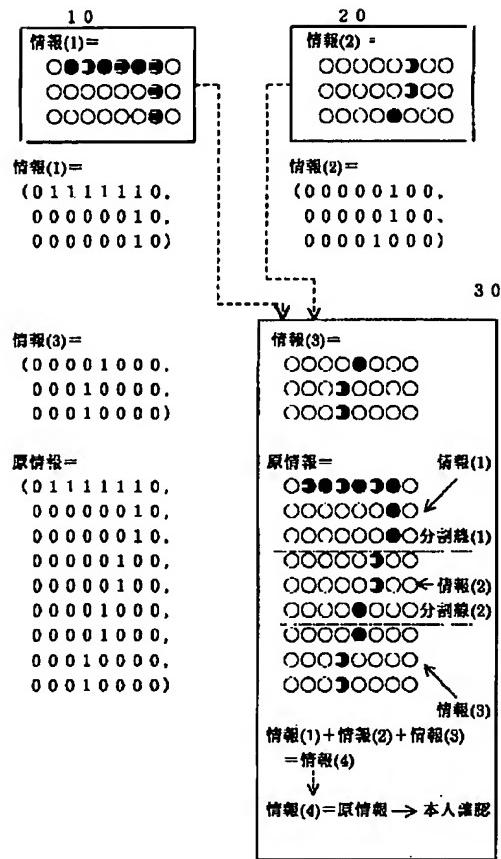
【図6】



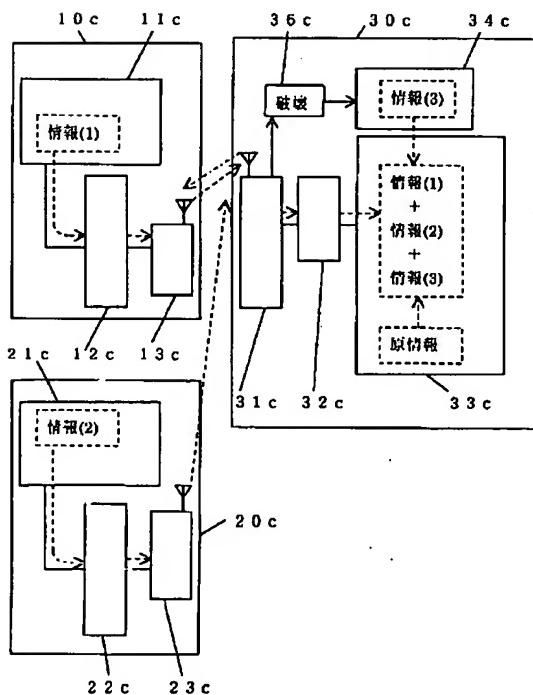
【図3】



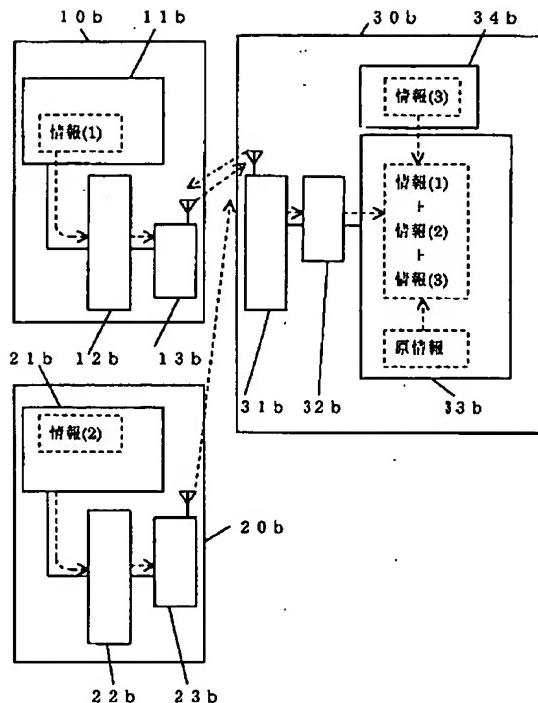
【図4】



【図7】



【図5】



---

フロントページの続き

(72)発明者 深津 博一  
名古屋市南区千種通2丁目13番地1 株式  
会社タイトック内

F ターム(参考) 3E040 AA10 CB01 DA02  
5B085 AE02 AE12 AE23  
5J104 AA07 KA01 NA05